Federal Public Key Infrastructure
Technical Working Group
Meeting Minutes

Prepared for the General Services Administration
By SRA International

Friday
March 25, 2015

1:00 p.m. – 2:30 p.m.

Teleconference

Time	Topic	Presenter
1:05	Welcome & Opening Remarks	Ola Bello
1:05	Microsoft Trust Store Program / Certificate Reputation Program	Jody Cloutier
1:35	High Speed PACS & Active Directory Smart Card Mapping	Tim Baldridge
2:20	Apple Over the Air Vulnerability	Carl Wallace
2:30	Adjourn	Ola Bello

Attendance List

Note: If you have any additions/corrections to the attendance list please let us know. Some people may not have responded to the roll call, or may not have identified their organization.

Name	Organization
Ambs, Matt	DHS
Anand, Neha	Symantec
Baldridge, Tim	DoD
Bello, Ola	FPKIMA
Blanchard, Debb	Verizon
Brown, Wendy	FPKIMA
Cimmino, Giuseppe	FPKIMA
Cloutier, Jody	Microsoft
Curtis, Dave	Treasury
DiSenia, Ridley	NASA
Edmunds, Debbie	State
Goss, Branden	NASA
Head, Derrick	DOS
Johnson, Todd	Treasury
Kane, Joe	USPS
McBride, Terry	Treasury
Monaghan, Jess	USPS
Myers, Kenneth	FPKIMA
Silver, Dave	GSA
Shomo, Larry	DHS
Wallace, Carl	DoD
Weiser, Russ	Verizon
Wood, Dan	Treasury

Welcome and Opening remarks (Ola Bello)

The FPKI TWG met via teleconference to receive three information presentations which could impact the Federal PKI (FPKI). Mr. Kenneth Myers informed the audience there was a last minute agenda change and the presentation by Mr. Tim Baldridge would be conducted first due to a scheduling conflict. Mr. Ola Bello opened the meeting and thanked everyone for calling in and gave a brief update of the TWG. Mr. Bello then turned it over to Mr. Tim Baldridge to discuss the next agenda item.

Agenda Item 1 – High Speed PACS Pilot and Active Directory Mapping (Tim Baldridge)

Mr. Baldridge representing the Department of Defense (DoD) presented two presentations on High Speed Physical Access Control Systems (PACS) Lessons Learned and Subject Name Mapping in Windows Smart Card Logon.

High Speed PACS Lessons Learned

The DoD is currently piloting Common Access Card (CAC) high speed contactless interfaces at different turnstile access points for “touch & go” CAC access. They are testing the use of Secure Messaging (SM) which is a simplified profile of a secure open protocol specified in the National Institute of Science and Technology (NIST) Special Publication (SP) 800-73-4 and the InterNational Committee for Information Technology Standards (INCITS) 504. Both are awaiting final approval. Each standard fully specify the contactless interface for full certificate usage and can manage all transactions other than card management over the contactless interface.

The benefit of using this standard is significant increase in validation speed ranging from 100 – 300 milliseconds compared to the 2 – 5 seconds currently experienced in enterprise PACS (EPACS). The speed advantage can only be achieved through an Elliptical Curve Cryptography (ECC) issuing CA and a Card Authentication Key (CAK) issued from this ECC CA. The CAK is the only interoperable 1-factor, strong authentication solution that also conducts revocation checking. Validation is only done to an “endorsement key” which is the PIV content signing key, this ties the key on the card to the cardholder. Currently Washington Metro Area Transit Authority (WMATA) has a proof of concept implementation using the CAC as a fare card. The CAK is linked to a backend funds accounting system so money amounts are not written to the card itself.

Active Directory Mapping

Mr. Baldridge presented a second topic on PIV subject name mapping to multiple windows accounts using the password hint function through a registry edit. There was general discussion on the purpose of mapping multiple PIV/CAC to one account (operations center use case) or mapping multiple accounts to one PIV/CAC (system admin use case). Mr. Baldridge said he has written a Windows PowerShell script to automate setup and can share it with anyone who wants to test it.

A question was asked if middleware or virtual software would support the hint function as well and there was a general response that it varies between products. Mr. Baldridge asked if any members were interested in writing a white paper to send to software providers to add this functionality to their products. Treasury, NASA, and DHS indicated they were interested in supporting the white paper development. Mr. Myers thanked Mr. Baldridge and then introduced Mr. Cloutier representing Microsoft for the next agenda item.

Action Item – Mr. Baldridge took an action with support from Treasury and DHS to develop a lessons learned white paper on how to map a PIV card to multiple logons using the security hint mechanism and how to get this is function with various middleware products.

Agenda Item 2 – Microsoft Trust Store Program (Jody Cloutier)

Mr. Cloutier apologized that he had a previous conflict during his new presentation time and would cede his agenda item back to the TWG. Mr. Myers apologized for the agenda change and informed the group this agenda item would be presented at the next TWG. Mr. Myers introduced Mr. Carl Wallace supporting DoD for the next agenda item.

Agenda Item 3 – Apple Over the Air (OTA) Vulnerability (Carl Wallace)

This presentation is limited only to installing certificates and private keys on Apple devices over the air to a mobile device management (MDM) service. The vulnerability presented is a weakness in:

1) The cryptography used by the Apple root CA (1024-bit key)
2) Apple root CA was expired but still issuing certificates
3) The method used by the Apple protocol (SCEP) to validate the device to/from the MDM was not binding the transaction to the device or the MDM
4) Apple root CA's can only be validated by name and date on the Apple website instead of through keys or hashes
5) The payload used during the registration process (P12) were not encrypted
6) The Apple protocol allows multiple ways of encoding the information transmitted and allows the encoding strategy to change during a single registration. Therefore a MITM can capture the SCEP, obtain the key and pass on a P12 format.

Mr. Wallace was able to conduct a successful man-in-the-middle (MITM) attack and compromise the registration session of multiple Apple devices. He also informed the group he has submitted a bug report to Apple who replied they investigated the issue and found it was not a vulnerability. The bug reported was submitted through the DoD

CIO office. If other agencies submit similar reports it may add weight to convince Apple they need to address this issue. The presentation was not shared and can be obtained by contacting Mr. Wallace directly. Mr. Myers thanked Mr. Wallace for his presentation.

The question was raised whether similar testing had been conducted with other devices such as Blackberry, Android, Microsoft, etc. Is the vulnerability inherent to the SCEP protocol or just the Apple implementation of MDM? Mr. Wallace said it was a factor of the manner in which the Apple over-the-air MDM was implemented and he had recommendations for the vulnerability could be mitigated.

Adjourn

Mr. Myers thanked everyone and asked if there were any questions. Mr. Baldridge suggested adjusting the meeting the time and length to a morning session on a day different than a Wednesday and making the meeting longer. Mr. Bello took the suggestion for consideration and thanked everyone for calling in.